Your Dose of IT Security Terms:

Cookie - Information placed on your computer when visiting a website, so as to remember something about you, should you re-visit the site.

Encryption - Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.

E-Shredder - A secure file deletion program that destroys electronic copies.

Firewall - An information technology (IT) security device, which is configured to permit, deny, or proxy data connections set and configured by the organization's security policy. Firewalls can either be hardware and/or software based.

Malicious Code - Software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic. Also referred to as Malware.

Patch - A small update released by a software manufacturer to fix bugs in existing programs.
Personally Identifiable Information (PII) - Refers to any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains.

Phishing - Pretending to be legitimate companies, while sending spam or pop-up messages to get you to reveal private or sensitive information.

Privacy - Set of fair information practices to ensure that an individual's personal information is accurate, secure, and current, and that individuals know about the uses of their data.

Public Key Infrastructure (PKI) - Enables users of a basically unsecured public network, such as the internet, to securely and privately exchange data and money through the use of a public and a private cryptographic key pair, obtained and shared through a trusted authority. It provides for a digital certificate that can identify an individual or organization and directory services that can store and, when necessary, revoke the certificates.

Scavenging - Searching through data residue in a system to gain unauthorized knowledge of sensitive data.

Social Engineering - A euphemism for non-technical or low-technology means - such as lies, impersonation, tricks, bribes, blackmail, and threats - used to attack information systems.

Spam - Electronic junk mail or junk newsgroup postings.

Spyware - computer software that collects personal information about users, without their informed consent.

Trojan Horse - A computer program that appears to have a useful function, but also has a hidden, and potentially malicious, function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity, which invokes the program.

Virus - A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting - i.e., inserting a copy of itself into and becoming part of - another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

Worm - A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

* Sources: http://www.sans.org/resources/glossary.php and Secure One HHS materials